

## Claims

1. (Currently Amended) A computer-implemented method for a computer-program module to provide application security threat-modeling, the method comprising:

responsive to a first user input, selecting a set of model components to represent respective elements of an application;

providing class definitions for the ~~a plurality of~~ model components to represent ~~respective elements of an application,~~ each class definition specifying a set of ~~potential~~ security threats associated with the model component;

responsive to a second user input, interconnecting at least a subset of the model components to form a logical model of the application;

~~marking one of the potential security threats associated with a selected model component as a countered security threat;~~

responsive to a third user input, selecting a particular component of the subset;

automatically analyzing the at least a subset of the model components to identify model components of the subset having a security threat associated with a substantially similar security threat category as one of the security threats associated with the particular component; and

~~automatically analyzing the at least a subset of model components and respective interconnections to identify a set of potential security threats corresponding to the at least a subset, the potential security threats being associated with one or more of the security threat categories; and~~

~~providing the identified set of potential security threats.~~

changing a manner in which the components are displayed to a user in response to the selection of the particular component and the analysis.

2. (Previously Presented) The method of claim 1, wherein the model components comprise a module, a port, a store, or a wire.

3. (Currently Amended) The method of claim 1, wherein the potential security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

4. (Currently Amended) The method of claim 1, wherein providing the class definitions further comprises determining the potential security threats based on functionality of the component with respect to the application.

5. (Currently Amended) The method of claim 1, wherein the security threats associated with the particular component are potential security threats ~~analyzing further comprises responsive to selection of a particular component of the model components, displaying each other component of the at least a subset that comprise at least a subset of similar potential security threats as the particular component.~~

6. (Currently Amended) The method of claim 1, wherein at least one of the security threats associated with the particular component is a countered security threat further comprising:

~~marking an additional potential security threat associated with a second selected component as a second countered security threat, wherein the second countered security threat and the countered security threat are substantially the same security threat;~~

~~wherein analyzing further comprises responsive to selection of the second selected component, automatically highlighting the selected component.~~

7. (Currently Amended) The method of claim 1, wherein analyzing further comprises providing for selection of a particular threat to indicate that the particular threat requires a threat mitigating implementation in a the particular model component of the at least a subset.

8. (Previously Presented) The method of claim 7, wherein providing for selection of the particular threat further comprises identifying a priority of the threat mitigating implementation.

9. (Previously Presented) The method of claim 7, wherein providing for selection of the particular threat further comprises identifying a desired level of strength of technology with which to mitigate the particular threat.

10. (Currently Amended) The method of claim 7, wherein providing for selection of the particular threat further comprises presenting information associated with a particular technology with which to mitigate the one or more ~~potential~~ security threats in a physical implementation of the application.

11. (Currently Amended) A computer-readable medium comprising computer-executable instructions for providing application security threat-modeling, the computer-executable instructions comprising instructions for:

defining a plurality of model components to represent respective elements of an application, each model component specifying a set of ~~potential~~ security threats associated with the component, the model components being defined with class definitions in a component schema, and the model components being selected in response to a first user input;

interconnecting, responsive to a second user input, at least a subset of the model components to form a logical model of the application;

~~marking one of the potential security threats associated with a selected model component as a countered security threat; and~~

selecting, responsive to a third user input, a particular component of the subset;

analyzing the at least a subset and respective interconnections to identify model components of the subset having a security threat associated with a substantially similar threat category as one of the security threats associated with the particular component; and ~~a set of potential security threats associated with associated ones of the security threat categories.~~

changing a manner in which the components are displayed to a user in response to the selection of the particular component and the analysis.

12. (Previously Presented) The computer-readable medium of claim 11, wherein the model components comprise a module, a port, a store, or a wire.

13. (Currently Amended) The computer-readable medium of claim 11, wherein the ~~potential~~ security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

14. (Currently Amended) The computer-readable medium of claim 11, wherein the security threats are potential security threats and wherein the computer-executable instructions for defining the model components further comprise instructions for determining the potential security threats for a component of the model components based on functionality of the component in the application.

15. (Currently Amended) The computer-readable medium of claim 11, wherein the security threats associated with the particular component are potential security threats ~~computer-executable instructions for analyzing further comprise instructions for:~~

~~responsive to selection of a particular component in the logical model, displaying each other component in the logical model that comprise at least a subset of similar potential security threats as the particular component.~~

16. (Currently Amended) The computer-readable medium of claim 11, wherein at least one of the security threats associated with the particular component is a countered security threat ~~the computer-executable instructions for analyzing further comprise instructions for:~~

~~marking an additional potential security threat associated with a second selected component as a second countered security threat, wherein the second countered security threat and the countered security threat are substantially the same security threat; and~~

~~responsive to selection of the second selected component automatically highlighting the selected component.~~

17. (Currently Amended) The computer-readable medium of claim 11, wherein the computer-executable instructions for analyzing further comprise instructions for providing for selection of a particular threat to indicate that the particular threat requires a threat mitigating implementation in a the particular component ~~of the logical model.~~

18. (Previously Presented) The computer-readable medium of claim 17, wherein the computer-executable instructions for providing for selection of the particular threat further comprise instructions for identifying a priority that corresponds to the threat mitigating implementation.

19. (Previously Presented) The computer-readable medium of claim 17, wherein the computer-executable instructions for providing for selection of the particular threat further comprise instructions for identifying a desired level of strength of technology with which to mitigate the particular threat.

20. (Currently Amended) The computer-readable medium of claim 17, wherein the computer-executable instructions for providing for selection of the particular threat further comprise instructions for presenting information associated with a particular technology with which to mitigate the one or more ~~potential~~ security threats in a physical implementation of the application.



21. (Currently Amended) A device comprising:

a memory comprising computer-executable instructions for providing application security threat-modeling;

a processor that is operatively coupled to the memory, the processor being configured to fetch and execute the computer-executable instructions from the memory, the computer-executable instructions comprising instructions for:

providing class definitions defining attributes of model components representing respective elements of an application, at least one attribute of the attributes associated with a model component specifying a set of potential security threats applicable to the model component, the model components being selected in response to a first user input;

presenting symbols associated with at least a subset of the model components on a display;

interconnecting respective ones of the at least a subset to form a logical model of the application;

~~marking one of the potential security threats associated with a selected model component as a countered security threat; and~~

responsive to a second user input, selecting a particular component of the subset;

analyzing the at least a subset of the model components to identify model components of the subset having a security threat associated with a substantially similar security threat category as one of the security threats associated with the particular component; and

changing a manner in which the components are displayed to a user in response to the selection of the particular component and the analysis.

~~analyzing the logical model in view of potential security threats associated with respective ones of the model components in the logical model to identify a set of potential security threats to the application.~~

22. (Previously Presented) The device of claim 21, wherein the model components comprise a module, a port, a store, or a wire.

23. (Currently Amended) The device of claim 21, wherein the potential security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation

24. (Currently Amended) The device of claim 21, wherein the computer-executable instructions for providing further comprise instructions for determining the potential security threats for a component of the model components based on functionality of the component in the application.

25. (Currently Amended) The device of claim 21, wherein the security threats associated with the particular component are potential security threats ~~the computer-executable instructions for analyzing further comprise instructions for responsive to selection of a particular component of the logical model, displaying each other component of the logical model that comprise at least a subset of similar potential security threats as the particular component.~~

26. (Currently Amended) The device of claim 21, wherein at least one security threats associated with the particular component is a countered security threat ~~the computer-executable instructions for analyzing further comprise:~~

~~instructions for marking an additional potential security threat associated with a second selected component as a second countered security threat, wherein the second countered security threat and the countered security threat are substantially the same security threat;~~

~~instructions responsive to selection of the second selected component, for automatically highlighting the selected component.~~

27. (Currently Amended) The device of claim 21, wherein the instructions for analyzing further comprise instructions for providing for selection of a particular threat to indicate that the particular threat requires a threat mitigating implementation in a the particular model component ~~of the logical model~~, the particular threat corresponding to the particular ~~model~~ component.

28. (Previously Presented) The device of claim 27, wherein the computer-executable instructions for providing for selection of the particular threat further comprise instructions for identifying a priority that corresponds to the threat mitigating implementation.

29. (Previously Presented) The device of claim 27, wherein the computer-executable instructions for providing for selection of the particular threat further comprise instructions for identifying a desired level of strength of technology with which to mitigate the particular threat.

30. (Currently Amended) The device of claim 27, wherein the computer-executable instructions for providing for selection of the particular threat further comprise instructions for presenting information associated with a particular technology with which to mitigate the one or more ~~potential~~ security threats in a physical implementation of the application.

31. (Currently Amended) A computing device comprising:

processing means for presenting a user interface for application security threat-modeling, the processing means comprising:

means for displaying and interconnecting a plurality of model components to design a logical model of an application, at least a subset of the model components comprising a corresponding set of potential security threat characteristics defined in a schema of class definitions for the model components;

means for specifying a component of the model components in the logical model;

means for analyzing the at least a subset of the model components to identify model components of the subset having a security threat associated with a substantially similar security threat category as one of the security threats associated with the specified component;

means for changing a manner in which the components are displayed in response to the specification of the particular component; and

~~means for identifying a set of potential security threats in view of one or more of module, port, store, or wire attributes associated with the at least a subset of model components that comprise the logical model; and~~

~~means for marking one of the potential security threats associated with a selected model component as a countered security threat;~~

means for selecting a particular solution to mitigate the potential security threats in the logical model.

32. (Canceled)

33. (Previously Presented) The computing device of claim 31, wherein the corresponding security threat characteristics comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

34. (Currently Amended) The computing device of claim 31, wherein the processing means further comprise means for selecting a priority that corresponds to the ~~potential~~ security threats.

35. (Currently Amended) The computing device of claim 31, wherein the means for selecting further comprise means for specifying a desired level of strength of technology with which to mitigate the ~~potential~~ security threats.

36. (Currently Amended) The computing device of claim 31, wherein the processing means further comprise means for selecting a particular technology with which to mitigate the ~~potential~~ security threats in a physical implementation of the application.

37. (Currently Amended) The method of claim 6 ~~claim 1~~, further comprising:

determining that the countered security threat neutralizes one of the ~~potential~~ security threats associated with a model component other than the ~~selected~~ particular model component; and

revising the set of ~~potential~~ security threats associated with at least one of model components other than the ~~selected-model~~ particular component by removing the neutralized ~~potential~~ security threat from the set.

38. (Currently Amended) The method of claim 37, further comprising automatically generating computer code configured to prevent the ~~potential security threat marked as the countered security threat in response to the marking.~~

39. (Currently Amended) The method of claim 16 ~~claim 11~~, further comprising instructions for:

determining that the countered security threat neutralizes one of the ~~potential~~ security threats associated with a model component other than the ~~selected model~~ particular component; and

revising the set of ~~potential~~ security threats associated with at least one of model components other than the ~~selected model~~ particular component by removing the neutralized ~~potential~~ security threat from the set.

40. (Currently Amended) The method of claim 39, further comprising instructions for automatically generating computer code configured to prevent the ~~potential security threat marked as the countered security threat in response to the marking.~~

41. (Currently Amended) The method of claim 26 ~~claim 21~~, wherein the computer-executable instructions further comprise instructions for:

determining that the countered security threat neutralizes one of the ~~potential~~ security threats associated with a model component other than the ~~selected model~~ particular component; and

revising the set of ~~potential~~ security threats associated with at least one of model components other than the ~~selected model~~ particular component by removing the neutralized ~~potential~~ security threat from the set.

42. (Currently Amended) The method of claim 41, wherein the computer-executable instructions further comprise instructions for automatically generating computer code configured to prevent the ~~potential security threat~~ ~~marked as the countered security threat in response to the marking.~~

43. (Canceled)

44. (Canceled)